REMARKS

This responds to the Office Action mailed on March 10, 2005.

No claims are amended, canceled, or are added; as a result, claims 1-15 remain pending in this application.

§103 Rejection of the Claims

Claims 1-15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shear et al (U.S. 6,157,721) in view of Santon et al. (U.S. 5,058,162).

Applicant respectfully traverses this rejection for the reasons set out below, and asks the Examiner for reconsideration.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Claims 3 and 10

US 6,157,721 (hereinafter: D1) discloses a "load module", preferably comprising one or more computer instructions and/or data elements used to assist, allow, prohibit, direct, control or facilitate at least one task performed at least in part by an electronic appliance such as a

computer (column 8, lines 18-24). A provider might produce a load module for use by a protected processing environment within a set top box or home media player. It could, for example, enable the set top box/home media player to play a movie (column 8, lines 43-48). A provider may provide, with each load module, associated specifications identifying the load module and describing the functions the load module performs (column 10, lines 7-11). A verifying authority uses an analysing tool to analyse and test a load module and determine whether it performs as specified by its associated specifications (column 10, lines 12-14). Once a verifying authority is satisfied with a load module, it affixes its digital seal of approval (column 10, lines 54-56). The digital sealing process is performed by creating a digital signature using a well-known process (column 10, lines 57-59). For this, a message digest may be encrypted using asymmetric key cryptography (column 13, lines 30-32). The load module and its associated digital signature are then delivered to the protected processing environment (column 14, lines 38-40). The protected processing environment decrypts the digital signature using a "second key" (column 14, lines 48-50), which has first securely been provided to it (column 13, lines 62-64).

US 5,058,162 (hereinafter: D2) discloses a method of distributing a plurality of data files to a plurality of recipients (abstract). Each is provided with a reading device, which may comprise a disk drive (column 7, lines 20-22). The drive is provided with conventional drive controller hardware and drive controller firmware. In addition, the drive is provided with a decryption chip (column 7, lines 32-37). The drive controller firmware comprises a second encryption key, a unique drive identifier and a security software program (column 7, lines 46-49). Identical copies of a secured media are supplied to a plurality of different software users (column 5, lines 9-12). A security system area contains various data used in implementing disk security (column 5, lines 51-52). A first region in the security system area contains a first encryption key. The security system area also contains a media edition identifier. The first encryption key which is stored in the first region of the security area is encrypted (column 6, lines 29-31). The remainder of the system area and the user data file area are encrypted using the first encryption key (in its unencrypted form). A region access map logically divides the user

data file area of the disk into a series of contiguous physical regions, for the purpose of identifying where data files assigned to various file groups are located (column 6, lines 44-48). The security software program is initiated by other drive controller firmware in response to the drive's reading of the security disk header of the disk. The security software program reads the second encryption key from the drive firmware (column 8, lines 30-32). The security software program provides the second encryption key to the decryption chip. Next, the security software program reads the encrypted first encryption key from the drive firmware and instructs the decryption chip to decrypt the first encryption key (column 8, lines 34-37). The security software program performs a validation operation using the media edition identifier. If the validation operation passes, the security provides the decryption chip with the first decryption key and instructs it to decrypt the region access map in the security area of the disk (column 8, lines 61-64).

Neither of D1 and D2 discloses a combination of features for a purpose similar to that of the invention defined in claim 3 of the present application. For the sake of argument, D1 will be taken as starting point for assessing the obviousness of the subject-matter of claim 3.

The system as claimed in claim 3 differs from the system known from D1 in that **D1 does not disclose** an input receiving protected contents containing secure device data comprising information required to decrypt the encrypted data, information on a protocol for communication between a content player and a secure device, and attribute data comprising information to find in the protected contents the appropriate protocol for communication between the content player and the secure device for retrieving information to decrypt the encrypted data. Consequently, **D1 also fails to teach** that the control device is programmed to use the attribute data to find the appropriate protocol information to establish a communication interface between the decryption device and a secure device used with the content player, or that the decryption device is suitable for communicating with the secure device as controlled by the protocol information to obtain information required to decrypt the encrypted data. Instead, the only encrypted data that is comprised in the load module 54 of D1 is the associated digital signature 106. The load module

is delivered to a protected processing environment, e.g. a secure device, not a control device. The protected processing environment uses a key securely provided first, in order to decrypt the digital signature (see column 13, lines 62-64 and column 14, lines 48-50). D1 describes using a (separate) secure key exchange protocol for this (column 13, lines 64-66). Thus, **D1 does not disclose that the contents contain information required to decrypt the encrypted data**.

The effect of this difference is that the system of claim 3 allows the content player to obtain the information to decrypt encrypted data with the aid of one of a plurality of secure devices, without first having to obtain information on the protocol needed to communicate with each of them. The objective problem solved by the present invention is thus to provide a system that enables content players to use one of a variety of types of secure devices to obtain the information needed to decrypt the encrypted data in the protected contents, and to do so in an efficient manner.

Faced with this problem, the skilled person would not turn to D2. Even if he were to combine the teachings of D1 and D2, which is strongly denied, he would not arrive at a system according to claim 3. D2 relates to a method of bundling a large number of different software programs on a single media, but to allow a customer access only to a small portion (column 1, lines 23-25 and 39-44). The disclosed system is a proprietary system that is tied to a particular type of device drive. Another reason that the skilled person would not combine the teachings of D1 and D2 is that the skilled person would not expect any advantage from such a combination. D1 is directed to techniques for certifying load modules (column 1, lines 25-28). D2 is directed to a method of distributing multiple data files on a distribution media, and to provide different software users with access to different sets of data files contained on the media. There is no advantage in combining the teachings, since certification of all the different sets of data files would be an unnecessary burden in view of the fact that a user only requires access to selected sets. Furthermore, additional certification would be redundant in the system of D2, since the unique code word provided by a distributor in D2 is based on the unique drive identifier assigned

to the drive of the software user (column 8, lines 6-7). Thus, the software user is already able to verify that the software does not originate from a 'rogue distributor'.

Even if the skilled person were to consult D2, he **would not find any disclosure of** protected contents containing information on a protocol for communication between a content player and a secure device for retrieving information to decrypt the encrypted data in the protected contents. Instead, D2 discloses that a software program in drive controller firmware (column 7, lines 46-48) provides a decrypted first encryption key to a decryption chip (column 8, lines 38-40). That is to say, the protocol information is incorporated in drive controller firmware, not on the disk 10 that contains the protected contents.

Because the combination of D1 and D2 fails to teach all elements of claim 3 and because the skilled person has anyway no reason or motivation to combine their teachings, it is submitted that the invention defined in claim 3 is not obvious. In view of the remarks above it is also submitted that claim 10 is not obvious.

Claims 1 and 15

It is submitted that the subject matter of claims 1 and 15 are not obvious in view of D1 and D2 for essentially the same reasons as given above for claim 3.

In particular, as set out above, **neither of D1 and D2 teaches protected contents containing attribute data comprising information to find in the protected contents the appropriate protocol for communication between the content player and the secure device for retrieving the information to decrypt the encrypted data**.

In view of the above, it is submitted that neither D1 nor D2 discloses all the limitations of claims and, accordingly, claims 1, 3, 10, and 15 are allowable. As claims 2, 4-9, 11-14 are dependent upon allowable claims they are also allowable.

In light of the above, Applicant respectfully submits that the rejection under 35 U.S.C. § 103 has been overcome, and withdrawal of this rejection is therefore respectfully requested.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney 408-278-4042 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

WILHELMUS GERARDUS PETRUS MOOIJ

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-278-4042

Date 05/16/08

By _____
Andre L. Marais
Reg. No. 48,095

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 16 day of May, 2005.

Dawn R. Shaw
Name

Dawn R. Shaw
Signature